What is claimed is:

1. An apparatus comprising:

an initialization storage to initialize a chipset in a secure environment for an isolated execution mode, the secure environment having a plurality of executive entities and being associated with an isolated memory area accessible by at least one processor, the at least one processor having a plurality of threads and operating in one of a normal execution mode and the isolated execution mode, the executive entities including a processor executive (PE) handler; and

a PE handler storage to store PE handler data corresponding to the PE handler, the PE handler data including a PE handler image to be loaded into the isolated memory area after the chipset is initialized, the loaded PE handler image corresponding to the PE handler.

2. The apparatus of claim 1 further comprises:

a thread count storage to store a thread count indicating number of threads currently operating in the isolated execution mode;

a thread count updater coupled to the thread count storage to update the thread count when the initialization storage is accessed;

a mode storage to store a chipset mode indicating a mode of operation of the chipset; and

a mode write circuit coupled to the mode storage to write the chipset mode to the mode storage.

3. The apparatus of claim 2 further comprising:

an identifier log storage to store identifiers of the executive entities operating in the isolated execution mode, the identifiers being read only when in lock;

a log lock storage to store a lock pattern indicating the identifiers in lock; and

a lock circuit coupled to the identifier log storage and the log lock storage to lock the identifiers based on the lock pattern.

4. The apparatus of claim 3 further comprising:

a fused key storage to store a fused key used in handling the executive entities; and

a scratch storage to store isolated settings used to configure the isolated execution mode.

5. The apparatus of claim 4 wherein the executive entities further include a processor executive (PE) and an operating system executive (OSE).

6. The apparatus of claim 5 wherein the chipset mode is one of an initialization waiting mode to indicate the chipset is waiting for initialization, a PE initialization in-progress mode to indicate the PE is being executed, a PE initialization completion mode to indicate the PE is completed, an OSE loaded mode to indicate the OSE has been loaded, a closing mode to indicate the isolated execution mode is closed, and a failure mode to indicate a failure.

7. The apparatus of claim 6 wherein the initialization storage returns an updated thread count when the chipset mode does not represent the failure mode and to return a current thread count when the chipset mode represents the failure mode, the updated thread count being one of an incremented thread count and a decremented thread count.

8. The apparatus of claim 7 wherein the initialization storage comprises:

an enrollment storage to return the incremented thread count when one of the threads enrolls in the isolated execution mode; and

a withdrawal storage to return the decremented thread count when one of the enrolled threads withdraws from the isolated execution mode.

9. The apparatus of claim 8 wherein the mode write circuit writes the chipset mode corresponding to a failure mode into the mode storage when the thread count reaches a thread limit.

10. The apparatus of claim 1 wherein the PE handler data further include a PE handler identifier, a PE handler size, and a PE handler address.

11. The apparatus of claim 6 wherein the PE handler storage is a non-volatile memory.

12. The apparatus of claim 6 wherein the fused key is returned when the fused key storage is read in the initialization waiting mode.

13. The apparatus of claim 12 wherein the fused key is programmed at manufacturing time to a random value.

14. The apparatus of claim 13 further comprising:

a status storage to store a status value of an isolated unlock pin used in restoring a root key from the fused key.

15. The apparatus of claim 4 wherein the isolated settings include an isolated base value, an isolated mask value, and a processor executive entry address, the isolated base and mask values defining the isolated memory area.

16. A method comprising:

initializing a chipset in a secure environment for an isolated execution mode by an initialization storage, the secure environment having a plurality of executive entities and being associated with an isolated memory area accessible by at least one processor, the at least one processor having a plurality of threads and operating in one of a normal execution mode and the isolated execution mode, the executive entities including a processor executive (PE) handler; and

storing PE handler data corresponding to the PE handler in a PE handler storage, the PE handler data including a PE handler image to be loaded into the isolated memory area after the chipset is initialized, the loaded PE handler image corresponding to the PE handler.

17. The method of claim 16 further comprises:

storing a thread count in a thread count storage indicating number of threads currently operating in the isolated execution mode;

updating the thread count when the initialization storage is accessed;

storing a chipset mode indicating a mode of operation of the chipset in a mode storage; and

writing the chipset mode into the mode storage.

18. The method of claim 17 further comprising:

storing identifiers of the executive entities operating in the isolated execution mode, the identifiers being read only when in lock;

storing a lock pattern indicating the identifiers in lock; and

locking the identifiers based on the lock pattern.

19. The method of claim 18 further comprising:

storing a fused key used in handling the executive entities in a fused key storage; and

storing isolated settings used to configure the isolated execution mode.

20. The method of claim 19 wherein the executive entities further include a processor executive (PE) and an operating system executive (OSE).

21. The method of claim 20 wherein the chipset mode is one of an initialization waiting mode to indicate the chipset is waiting for initialization, a PE initialization in-progress mode to indicate the PE is being executed, a PE initialization completion mode to indicate the PE is completed, an OSE loaded mode to indicate the OSE has been loaded, a closing mode to indicate the isolated execution mode is closed, and a failure mode to indicate a failure.

22. The method of claim 21 wherein initializing the chipset comprises

returning an updated thread count when the chipset mode does not represent the failure mode, the updated thread count being one of an incremented thread count and a decremented thread count; and

returning a current thread count when the chipset mode represents the failure mode.

23. The method of claim 22 wherein initializing the chipset further comprises:

returning the incremented thread count when one of the threads enrolls in the isolated execution mode; and

returning the decremented thread count when one of the enrolled threads withdraws from the isolated execution mode.

24. The method of claim 23 wherein writing the chipset mode comprises writing the chipset mode corresponding to a failure mode when the thread count reaches a thread limit.

25. The method of claim 16 wherein the PE handler data further include a PE handler identifier, a PE handler size, and a PE handler address.

26. The method of claim 21 wherein the PE handler storage is a non-volatile memory.

27. The method of claim 21 wherein the fused key is returned when the fused key storage is read in the initialization waiting mode.

28. The method of claim 27 wherein the fused key is programmed at manufacturing time to a random value.

29. The method of claim 28 further comprising:

storing a status value of an isolated unlock pin used in restoring a root key from the fused key.

30. The method of claim 19 wherein the isolated settings include an isolated base value, an isolated mask value, and a processor executive entry address, the isolated base and mask values defining the isolated memory area.

31. A computer program product comprising:

a machine useable medium having computer program code embedded therein, the computer program product having:

computer readable program code for initializing a chipset in a secure environment for an isolated execution mode by an initialization storage, the secure environment having a plurality of executive entities and being associated with an isolated memory area accessible by at least one processor, the at least one processor having a plurality of threads and operating in one of a normal execution mode and the isolated execution mode, the executive entities including a processor executive (PE) handler; and

computer readable program code for storing PE handler data corresponding to the PE handler in a PE handler storage, the PE handler data including a PE handler image to be loaded into the isolated memory area after the chipset is initialized, the loaded PE handler image corresponding to the PE handler.

32. The computer program product of claim 31 further comprises:

computer readable program code for storing a thread count in a thread count storage indicating number of threads currently operating in the isolated execution mode;

computer readable program code for updating the thread count when the initialization storage is accessed;

computer readable program code for storing a chipset mode indicating a mode of operation of the chipset in a mode storage; and

computer readable program code for writing the chipset mode into the mode storage.

33. The computer program product of claim 32 further comprising:

computer readable program code for storing identifiers of the executive entities operating in the isolated execution mode, the identifiers being read only when in lock;

computer readable program code for storing a lock pattern indicating the identifiers in lock; and

computer readable program code for locking the identifiers based on the lock pattern.

34. The computer program product of claim 33 further comprising:

computer readable program code for storing a fused key used in handling the executive entities in a fused key storage; and

computer readable program code for storing isolated settings used to configure the isolated execution mode.

35. The computer program product of claim 34 wherein the executive entities further include a processor executive (PE) and an operating system executive (OSE).

36. The computer program product of claim 35 wherein the chipset mode is one of an initialization waiting mode to indicate the chipset is waiting for initialization, a PE initialization in-progress mode to indicate the PE is being executed, a PE initialization completion mode to indicate the PE is completed, an OSE loaded mode to indicate the

OSE has been loaded, a closing mode to indicate the isolated execution mode is closed, and a failure mode to indicate a failure.

37. The computer program product of claim 36 wherein the computer readable program code for initializing the chipset comprises

computer readable program code for returning an updated thread count when the chipset mode does not represent the failure mode, the updated thread count being one of an incremented thread count and a decremented thread count; and

computer readable program code for returning a current thread count when the chipset mode represents the failure mode.

38. The computer program product of claim 37 wherein the computer readable program code for initializing the chipset further comprises:

computer readable program code for returning the incremented thread count when one of the threads enrolls in the isolated execution mode; and

computer readable program code for returning the decremented thread count when one of the enrolled threads withdraws from the isolated execution mode.

39. The computer program product of claim 38 wherein the computer readable program code for writing the chipset mode comprises computer readable program code for writing the chipset mode corresponding to a failure mode when the thread count reaches a thread limit.

40. The computer program product of claim 31 wherein the PE handler data further include a PE handler identifier, a PE handler size, and a PE handler address.

41. The computer program product of claim 36 wherein the PE handler storage is a non-volatile memory.

42. The computer program product of claim 36 wherein the fused key is returned when the fused key storage is read in the initialization waiting mode.

43. The computer program product of claim 42 wherein the fused key is programmed at manufacturing time to a random value.

44. The computer program product of claim 43 further comprising:

computer readable program code for storing a status value of an isolated unlock pin used in restoring a root key from the fused key.

45. The computer program product of claim 34 wherein the isolated settings include an isolated base value, an isolated mask value, and a processor executive entry address, the isolated base and mask values defining the isolated memory area.

46. A system comprising:

at least one processor having a plurality of threads and operating in one of a normal execution mode and an isolated execution mode;

a memory having an isolated memory area accessible to the at least one processor in the isolated execution mode; and

a chipset circuit coupled to the at least one processor and the memory comprising:

an initialization storage to initialize a chipset in a secure environment for the isolated execution mode, the secure environment having a plurality of

executive entities and being associated with the isolated memory area, the executive entities including a processor executive (PE) handler, and

a PE handler storage to store PE handler data corresponding to the PE handler, the PE handler data including a PE handler image to be loaded into the isolated memory area after the chipset is initialized, the loaded PE handler image corresponding to the PE handler.

47. The system of claim 46 wherein the chipset circuit further comprises:

a thread count storage to store a thread count indicating number of threads currently operating in the isolated execution mode,

a thread count updater coupled to the thread count storage to update the thread count when the initialization storage is accessed;

a mode storage to store a chipset mode indicating a mode of operation of the chipset; and

a mode write circuit coupled to the mode storage to write the chipset mode into the mode storage.

48. The system of claim 47 wherein the chipset circuit further comprises:

an identifier log storage to store identifiers of the executive entities operating in the isolated execution mode, the identifiers being read only when in lock;

a log lock storage to store a lock pattern indicating the identifiers in lock; and

a lock circuit coupled to the identifier log storage and the log lock storage to lock the identifiers based on the lock pattern.

49. The system of claim 48 wherein the chipset circuit further comprises:

a fused key storage to store a fused key used in handling the executive entities; and

a scratch storage to store isolated settings used to configure the isolated execution mode.

50. The system of claim 49 wherein the executive entities further include a processor executive (PE) and an operating system executive (OSE).

51. The system of claim 50 wherein the chipset mode is one of an initialization waiting mode to indicate the chipset is waiting for initialization, a PE initialization in-progress mode to indicate the PE is being executed, a PE initialization completion mode to indicate the PE is completed, an OSE loaded mode to indicate the OSE has been loaded, a closing mode to indicate the isolated execution mode is closed, and a failure mode to indicate a failure.

52. The system of claim 51 wherein the initialization storage returns an updated thread count when the chipset mode does not represent the failure mode and to return a current thread count when the chipset mode represents the failure mode, the updated thread count being one of an incremented thread count and a decremented thread count.

53. The system of claim 52 wherein the initialization storage comprises:

an enrollment storage to return the incremented thread count when one of the threads enrolls in the isolated execution mode; and

a withdrawal storage to return the decremented thread count when one of the enrolled threads withdraws from the isolated execution mode.

54. The system of claim 53 wherein the mode write circuit writes the chipset mode corresponding to a failure mode into the mode storage when the thread count reaches a thread limit.

55. The system of claim 46 wherein the PE handler data further include a PE handler identifier, a PE handler size, and a PE handler address.

56. The system of claim 51 wherein the PE handler storage is a non-volatile memory.

57. The system of claim 51 wherein the fused key is returned when the fused key storage is read in the initialization waiting mode.

58. The system of claim 57 wherein the fused key is programmed at manufacturing time to a random value.

59. The system of claim 58 wherein the chipset circuit further comprises:

a status storage to store a status value of an isolated unlock pin used in restoring a root key from the fused key.

60. The system of claim 49 wherein the isolated settings include an isolated base value, an isolated mask value, and a processor executive entry address, the isolated base and mask values defining the isolated memory area.